Gerenc.tecnol.inform. Vol 6|No 16|31-40,2007

# ESTEGANOGRAFÍA EN DISPOSITIVOS MÓVILES

**AUTOR**
Gabriel Alejandro Gómez
Ingeniero de Sistemas
Pontifica Universidad Javeriana
g.gomez@javeriana.edu.co
COLOMBIA

**AUTOR**
Juliana Valdés Jácome
Ingeniera de Sistemas
Pontifica Universidad Javeriana
valdesj@javeriana.edu.co
COLOMBIA

***Fecha de Recepción : 16 de Sept de 2007***

***Fecha de Aceptación : 13 de Nov de 2007***

***Articulo tipo 1***

## RESUMEN.

*El artículo presenta una síntesis de la investigación titulada Esteganográfia en dispositivos móviles. Para el desarrollo de ésta se revisaron temas generales como manipulación de imágenes, técnicas esteganográficas y algoritmos esteganográficos; orientado al ocultamiento de información al interior de imágenes en formato real RGB (Red, Green, Blue). De igual manera, se realizo un análisis que permitiera utilizar las propiedades innatas de movilidad, portabilidad y recursos multimedia de los dispositivos móviles para incorporarlos a un modelo de aseguramiento de información basado en esteganográfia. Como resultado de la investigación se obtuvo un modelo esteganográfico de transmisión de datos capaz de enviar y recibir información oculta al interior de una fotografía capturada con el dispositivo móvil. La capa lógica (agrupación de módulos que sintetizan el modelo esteganográfico propuesto) es la encargada de realizar el proceso de forma transparente para el usuario sirviendo de intermediaria entre el usuario y los recursos ofrecidos por el dispositivo móvil. Al interior del núcleo de procesamiento se cuenta con dos algoritmos esteganográficos que atacan el objetivo de ocultamiento de manera secuencial o aleatoria. Si bien, los dos algoritmos operan de forma diferente, el proceso de inserción se basa en la misma operación: Inserción en el BIT menos significativo. Debido al carácter estándar del modelo propuesto este es portable a cualquier tipo de dispositivo móvil que cumpla los requisitos solicitados.*

**PALABRAS CLAVES**

Esteganográfia
Dispositivos Móviles
Ocultamiento de información
Modelo esteganográfico
Seguridad informatica

**ABSTRACT**

The article presents a synthesis of the research investigation entitled Steganography on mobile devices. General topics such as image manipulation, Steganographic techniques and Steganography algorithms; oriented to the concealment of information inside images in RGB format (Red, Green, Blue) were researched. An analysis of the innate properties of

mobility, portability and multimedia resources found on mobile devices led to the proposal of an information assurance model based on Steganography. The proposed Steganographic model for data transmission is capable of sending and receiving hidden data inside a photograph captured by the mobile device. The logical layer (grouping of modules that summarize the Steganographic model proposed) is responsible for carrying out the process in a transparent manner serving as an intermediary between the user and the resources offered by the mobile device. Inside the processing core are two Steganographic algorithms that attack the problem of concealing the information either sequentially or randomly inside the photograph. Even thought both algorithms work in a different way, the insertion process is based on the same operation: less significant BIT insertion. The proposed model is usable in any mobile device that meets the requirements thanks to its generic design.

**KEYWORDS**

Steganography
Mobile devices
Data hiding
Information security
Steganographic model

**INTRODUCCIÓN**

La búsqueda de seguridad en la información ha motivado a los seres humanos a buscar innumerables maneras de protegerla. Desde tiempos inmemoriales se utilizaron diversas técnicas para el envío de mensajes entre poblaciones o regiones apartadas.

En la actualidad, el afán por proteger la información ha llevado a nuevos niveles la manera en la que ella se transmite y oculta. Algunas técnicas de protección incluyen la criptografía [15] y la esteganográfia [1, 2] como métodos para enviar información sin que su contenido se vea comprometido en caso de ser interceptada por terceros no autorizados.

El artículo presenta el modelo que, usando esteganográfia, permite la transmisión de información oculta a través de dispositivos móviles usando como medio la red celular. Dicho modelo (capa lógica) hará las veces de tramitador de información al interior del dispositivo móvil realizando los procesos necesarios que permiten que el proceso sea transparente para el usuario.

Utilizando las capacidades ofrecidas por las librerías Wireles Messaging Api (WMA 2.0 - JSR 205 [12]), PushRegistry y Application Management System(AMS) ofrecidos a través de Mobile Information Device Profile (MIDP 2.0 - JSR 118 [13]) y Mobile Media Api (MMAPI - JSR 135 [14]) propios de la plataforma especializada Java Micro Edition (JME) se logro la implementación de un prototipo funcional del modelo propuesto.

El documento se encuentra dividido de la siguiente forma: la sección uno (1) presenta una breve documentación acerca del estado del arte en el campo de la esteganográfia, particularmente en dispositivos móviles; la sección dos (2) explica el proceso de análisis y diseño y las funcionalidades mínimas que debe proporcionar el modelo propuesto; seguidamente, en la sección tres (3), se expone el modelo desarrollado; para en la ultima sección presentar las conclusiones.

## 1. ESTEGANOGRÁFIA Y DISPOSITIVOS MÓVILES

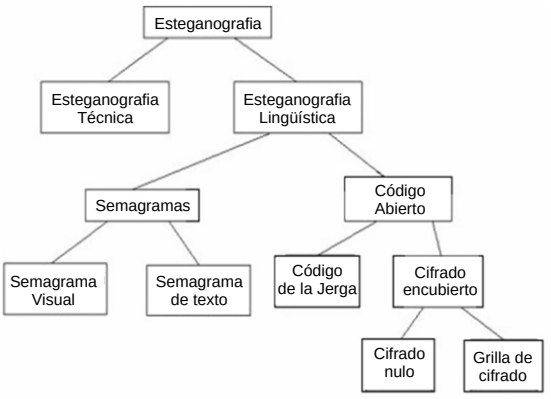
La esteganográfia se define como el arte de ocultar información dentro de portadores aparentemente inofensivos [11]. Su propósito busca que la información oculta en el portador o carrier, sea indetectable frente a terceros que pretenden manipular los datos, sean para fines legales o ilegales. En caso de ser localizada, existen procedimientos adecuados o herramientas de software que permiten la extracción de esta información.

### 1.1 Técnicas esteganográficas.

Durante la Primera y Segunda Guerra Mundial, se produjeron avances significativos en el campo de la esteganografía; técnicas como cifrado nulo, micro-puntos, entre otros, fueron técnicas que comenzaron a fortalecerse. A continuación, se presenta una taxonomía común de dichas técnicas (ver Figura 1):

- Esteganográfia técnica: Utiliza métodos científicos, tal como el uso de la tinta invisible, micro puntos u otros métodos de tamaño reducido, para ocultar mensajes.

**Figura 1. Clasificación de las Técnicas de Esteganográfia. Adaptada de Gary C. Kessler [1]**



- Esteganográfia lingüística: Oculta información, de forma no obvia, en el portador. De forma más categórica se visualiza como semagrama o código abierto.

- Semagrama: Oculta información utilizando símbolos o signos.

- Semagrama visual: Utiliza objetos físicos del contexto visual cotidiano para dar a entender el mensaje (forma intrínseca).

- Semagrama de Texto: Oculta información modificando la apariencia del texto portador.

- Código Abierto: Oculta información, de manera no obvia para un observador incauto, al interior de un mensaje portador legitimo. El mensaje portador es llamado mensaje abierto, mientras el mensaje oculto es conocido como mensaje secreto.

- Código de la Jerga: Como su nombre lo indica, utiliza un lenguaje comprendido por un cierto grupo de personas, que carece de sentido para otras, para ocultar información.

- Cifrado en cubierto o de ocultamiento: Ocultan información a la luz de la vista y de quien observa el mensaje portador. Solo quien tenga conocimiento del proceso seguido para el ocultamiento podrá recuperar el mensaje, realizando el proceso inverso.

- Grilla de Cifrado: Oculta información empleando una plantilla con orificios a través de los cuales aparece el mensaje oculto. El mensaje portador contiene un mensaje abierto el cual, al colocar la plantilla sobre este, tapa el texto no importante y deja en los orificios las palabras que hacen parte del mensaje oculto.

- Cifrado Nulo: Oculta información utilizando un grupo de reglas preestablecidas.

Cada técnica mencionada utiliza metodologías particulares que las hacen más, o menos apetecidas para determinados usos. Las firmas digitales o marcas de agua son ejemplo de uso de esteganográfia en el mundo real.

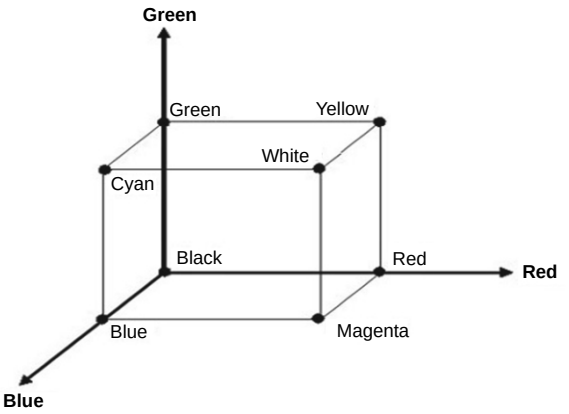
### 1.2 Esteganográfia en imagenes

Los mensajes codificados en imágenes digitales son los más utilizados en la actualidad. Debido a la limitada capacidad de visión que posee el sistema visual humano, los cambios realizados sobre la imagen, generalmente, no son percibidos por el ojo humano y pasan inadvertidos. Todo texto plano, texto cifrado, imagen u otro medio que pueda ser codificado como flujo de bits, puede ocultarse al interior de una imagen digital.

Para realizar un completo estudio de la esteganográfia en imágenes, se debe analizar lo siguiente: composición (color) de las imágenes, procedimientos para desarrollar procesos de esteganográfia y formatos de imágenes en los cuales es viable o no ocultar información. Puesto que el modelo esteganográfico proyectado se limita a imágenes como archivos portadores no se hace mención de esteganográfia sobre otro tipo de archivo.

Como se puede observar en la Figura 2 (RGB Cube), los colores se encuentran representados de acuerdo a la intensidad de cada uno de los colores primarios: rojo, verde y azul.

**Figura 2. El Cubo de colores RGB. Adaptado de Gary C. Kessler [1]**

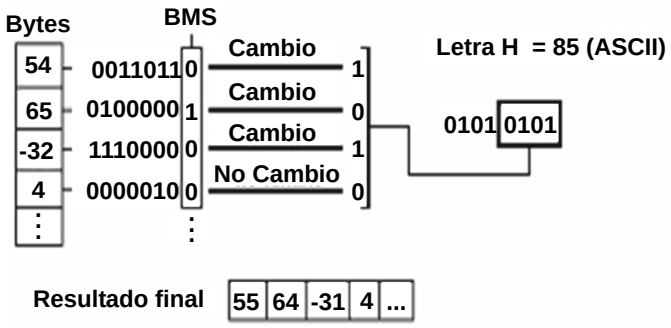



Así como las imágenes digitales se encuentran representadas por píxeles; estos píxeles se encuentran conformados por la estructura de colores RGB (Red, Green, Blue). Cada componente RGB se encuentra especificado por un único byte (8 bits), de modo que los valores para cada nivel de color se encuentran representados de 0 a 255.

Una vez analizada la composición (color) de las imágenes, se procede a analizar los procesos de esteganográfia. El modelo generalizado para realizar esteganográfia en imágenes se basa en el procedimiento de nombre Inserción en Bit Menos Significativo o LSB (por sus siglas en ingles: Less Significant Bit) [2]. El BIT menos significativo es el BIT cuyo valor representa el cambio de menor valor en la notación binaria utilizada para presentar la composición de un objeto o dato. El proceso de inserción utiliza la representación binaria del mensaje a ocultar para sobrescribir el BIT menos significativo de cada byte / unsigned int(dos bytes) que componen el archivo

portador o parte de este. La figura 3 muestra este procedimiento.

**Figura 3. Inserción en bit menos significativo de un arreglo de Bytes.**




Debido a los diferentes formatos de imágenes existentes, es imposible hablar de un trato generalizado para todos. Si bien toda imagen se compone de bytes, cada formato utiliza una estructura única para ordenar, comprimir y persistir la información. Debido a lo anterior, la esteganográfia propone dos unidades fundamentales para realizar el ocultamiento de información. Si bien no son las únicas, son las más usadas.

### 1.3 Unidad fundamental

A continuación se presentan las dos unidades fundamentales mas utilizadas en lo que a esteganográfia sobre imágenes concierne.

#### 1.3.1 Pixel

El Píxel [3] es la unidad fundamental de toda imagen digital. Se encuentra conformado por la estructura de colores representada por los canales RGB. Dependiendo de la profundidad seleccionada (1 a 48 bits), cada canal podrá contar con un bit o hasta 2 bytes para representar la gama de variaciones que el canal puede producir. La combinación de los tres canales produce el color final según el espectro de colores determinado.

Utilizando el píxel como unidad fundamental para realizar el ocultamiento, el proceso IBMS cambia el bit menos significativo del canal seleccionado provocando un cambio de 1/2número de bits que componen el canal sobre el canal y a su vez de 1/2 profundidad sobre la totalidad del color de píxel.

#### 1.3.2 Coeficientes Cuantificados

Son la unidad fundamental de imágenes que utilizan transformadas Discreta de Coseno, *Fourier*[4] o *Wavelet*[5] para migrar el espacio del color tradicional RGB a espacios como *YcbCr* (Por sus siglas en ingles: *Luminance* (Luminancia - escala de grises) *Crominance* X 2 (dos componentes de croma - color)), utilizado por JPEG. Dichos coeficientes son ordenados en una matriz para luego ser manipulados según cada uno de los estándares mencionados para comprimir y persistir la información.

Sin importar el formato de la imagen, los coeficientes cuantificados son el resultado de aplicar una tabla de cuantificación o los coeficientes obtenidos de la transformada. Es a dicho coeficientes que le es aplicado el proceso de cambio BIT menos significativo.

### 1.4 Modelos base

La esteganográfia propone distintos modelos base para realizar el proceso de ocultamiento de una forma particular. A continuación se presentan los dos modelos utilizados.

#### 1.4.1 Modelo Lineal Secuencial

Propone un esquema de esteganográfia basado en el ocultamiento lineal de la información a través de la superficie de la imagen. El modelo propone como punto de inicio el primer o último píxel/coeficiente cuantificado de la imagen. Desde este punto en adelante (o hacia atrás, según sea el caso) se realiza un recorrido lineal y secuencial sobre la superficie de la imagen ocultando la información mediante IBMS.

#### 1.4.2 Modelo Pseudo aleatorio con llave

Propone un esquema de esteganográfia basado en la generación de números aleatorios utilizando como semilla una llave dada. Los números aleatorios generados servirán como mapa de navegación a través de la superficie de la imagen permitiendo aplicar IBMS sobre diferentes coordenadas de píxeles a lo largo y ancho de la imagen.

### 1.5 Esteganográfia en dispositivos móviles

En la actualidad, la esteganográfia es usada masivamente en ordenadores convencionales; pero poco tratada en el área de dispositivos móviles.

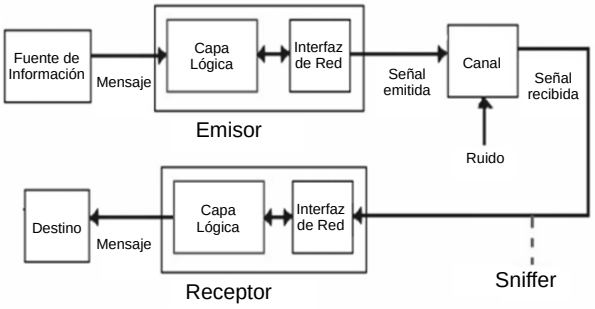
*Fujitsu*, compañía europea que ofrece servicios TI en Europa, Medio Oriente y África (para más información acerca de la compañía remítase a [9]) es la compañía pionera en el área de la esteganográfia orientada a dispositivos móviles [10]. Su funcionamiento se basa en la escritura de códigos no visibles impresos sobre papel los cuales son leídos utilizando como lector un dispositivo móvil, ya sea teléfono celular o PDAs. La imagen capturada es enviada por el dispositivo a un servidor el cual procesa la imagen y envía el resultado al

dispositivo emisor. Debido al carácter propietario es poca la información que se posee acerca de este tipo de tecnología e implementación.

## 2. MODELO ESTEGANOGRÁFICO DETRANSMISIÓN DE DATOS PARA DISPOSITIVOS MÓVILES

En el proceso esteganográfico intervienen un emisor y un receptor entre los cuales se da una comunicación a través del medio escogido por los dos, en este caso, la red de comunicación celular (Figura 4). El modelo esteganográfico de transmisión de datos implementado tiene como fin representar por módulos cada uno de los procesos fundamentales entre las partes para realizar el proceso de ocultamiento y retoma de datos.

**Figura 4. Integración del Modelo de comunicación con el modelo esteganográfico (capa lógica).**




El modelo se encuentra divido en dos formas de ejecución fundamentales:

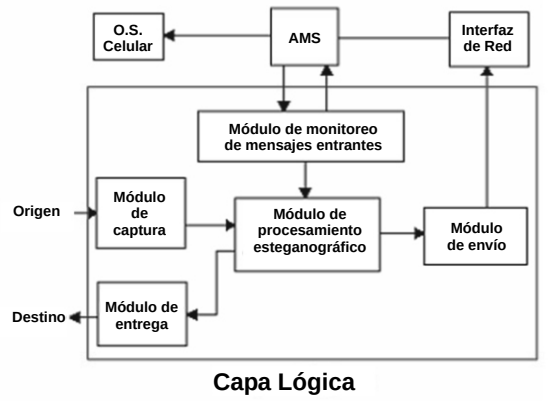
- **Envío:** El emisor oculta información al interior de una imagen portadora (capturada a través del dispositivo) y la envía a un receptor.
- **Recepción:** El receptor recibe, a través del canal, la imagen portadora con información oculta en su interior.

Dependiendo del rol ejecutado por cada parte, esta puede ser emisor o receptor según aplique.

Como forma de agrupar las tareas desarrolladas para el proceso se plantea la creación de una capa lógica la cual funciona como proceso intermedio al interior del emisor y receptor. La interacción entre dichos componentes será la encargada de producir el producto final.

La capa lógica se encuentra ubicada en cada uno de los extremos de la comunicación (emisor, receptor) puesto que es esta la encargada de realizar de captura, ocultamiento, envío y recepción de un mensaje procesado con esteganográfia desde y hacia el destino (Figura 5). Debido a lo anterior, es imperativo que cada una de las partes posea tanto el conocimiento como la tecnología y el software necesario para realizar el proceso de ocultamiento, así como su inverso.

**Figura 5. Módulos que componen el modelo de transmisión esteganográfico (capa lógica)**




Se debe traer a conocimiento que todos los procesos realizados al interior de cada uno de los módulos, es realizado en la memoria volátil del dispositivo como medida antiforense.

### 2.1 Módulo de captura

Es el punto de entrada en la modalidad de envío. El módulo de captura se especializa en la recolección y estructuración de la información necesaria para realizar el proceso de esteganográfia. Para tal fin provee interfaces para la captura de mensaje y número celular de destino. De igual forma, es la encargada de acceder las capacidades multimedia del dispositivo, a través de los métodos proveídos por la librería MMAPI (*Mobile Media Api* - JSR 135), para capturar la imagen portadora en formato PNG.

Terminado el proceso de captura, imagen portadora y mensaje huésped ingresan al módulo de procesamiento. El número telefónico al cual se encuentra dirigido el mensaje es ingresado directamente al módulo de envío debido a que este no hace parte de la información a ser ocultada.

### 2.2 Módulo de procesamiento esteganográfico

El módulo de procesamiento es el encargado de realizar el proceso esteganográfico. Su operación esta dividida en dos modos de ejecución.

- **Envío:** En la modalidad de envío se realiza el proceso de inserción del mensaje huésped al archivo portador. Utilizando uno de los dos algoritmos[1] proveídos se procede a realizar el proceso de ocultamiento del encabezado[2] y mensaje que se desea enviar al interior de la fotografía capturada. La imagen resultante del proceso (imagen portadora) ingresa al modulo de envío

- **Recepción:** Aplicando un esquema de grilla de píxeles se procede a la extracción del encabezado. Al interior del encabezado[3] se encuentra el marcador de algoritmo de esteganográfia utilizado así como el tamaño de la imagen, tamaño del mensaje y demás datos necesarios para inicializar el modulo de procesamiento esteganográfico en modo de operación inverso. Dicho marcador determina la forma en que el algoritmo deberá operar para recuperar la información concerniente al mensaje oculto.

### 2.3 Módulo de envío

El módulo de envío se especializa en agrupar los elementos del proceso a través del formato estándar MMS (*Multimedia Messaging System*). El mensaje MMS es construido a partir del numero celular ingresado en el modulo de captura así como el puerto (*ApplicationId*) que el modulo de monitoreo de mensajes escucha. Como carga útil del mensaje se adiciona la imagen en formato PNG, portadora del mensaje oculto.

Una vez construido, el mensaje MMS es enviado a través del canal utilizando la interfaz de red del dispositivo móvil.

### 2.4 Módulo de monitoreo de mensajes entrantes

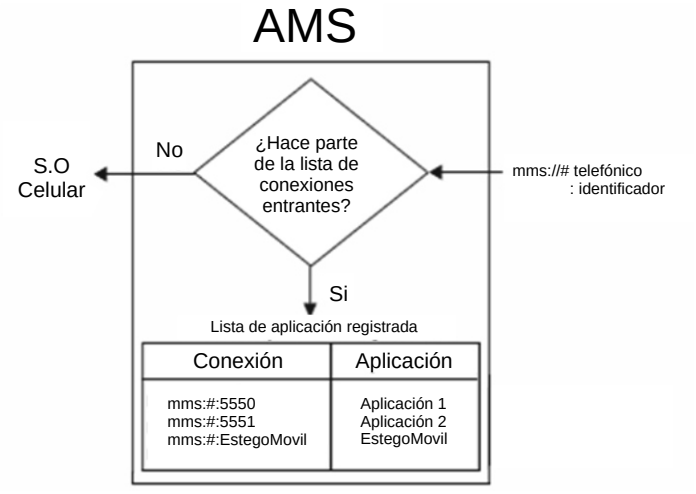
El módulo de monitoreo de mensaje entrantes se especializa en la recepción de mensajes dirigidos a la capa lógica en sus dos modalidades de ejecución (envío y recepción). Su registro es realizado en tiempo de instalación y en tiempo de ejecución de la aplicación.

En tiempo de instalación en el dispositivo móvil, la capa lógica se registra ante el AMS (Application Management System) como dueña de toda comunicación entrante que contenga el identificador (ApplicationId) designado para la aplicación (Figura 6).

1.La descripción detallada de los algoritmos se puede apreciar en la sección 3.2.
2.La descripción detallada de los componentes del encabezado se puede apreciar en el capitulo 3.1.

Realizar este registro permite, a través del comando pushregistry, ejecutar la capa lógica de forma automática al arribar un mensaje multimedia dirigido a esta.

**Figura 6. Funcionamiento de Application Management System (AMS)**




En tiempo de ejecución, el módulo de recepción instaura un lector de flujos encargado de recolectar los mensajes entrantes. El lector colocado por la capa lógica determina, según el puerto marcado al interior del mensaje MMS, si dicho mensaje es dirigido a esta. Si el mensaje no se encuentra dirigido a la capa lógica, esta lo ignora y permite que el sistema operativo del dispositivo maneje el evento. Por el contrario, si el mensaje esta dirigido a la capa lógica esta lo recibe y sube la bandera en el procesador esteganográfico para que comience su operación de forma inversa.

El lector instaurado funciona en los dos modos de operación. En modo de envío escucha posibles mensajes entrantes. En modo de recepción, el lector es el encargado de entregar el mensaje al módulo de procesamiento para realizar el proceso esteganográfico inverso. Si un mensaje arriba durante la realización del proceso de envío, el lector, de forma inmediata, cambia el modo de ejecución a receptor anulando el procedimiento de envío y devolviéndolo ha su estado inicial.

### 2.5 Módulo de entrega de mensaje

El módulo de entrega se especializa en mostrar al usuario la información obtenida del mensaje MMS a través del módulo de procesamiento esteganográfico.

El mensaje huésped extraído así como la imagen

portadora son el producto final de la capa lógica así como del módulo de entrega. Ambos son desplegados al usuario receptor para su lectura y análisis. El destinatario recibe el mensaje enviado por el emisor de forma transparente.

## 3. PROTOTIPO ESTEGOMOVIL

EstegoMovil es un prototipo que implementa el modelo propuesto en la sección dos (2). Se encarga de transferir información oculta entre dos usuarios utilizando los algoritmos de esteganográfia propuestos, con el fin de proporcionar confidencialidad a los datos que se transmiten. Para ello, el programa permite al usuario enviar o recibir información, usando como medio de transmisión la red de telefonía celular. Con EstegoMovil se pretende presentar la efectividad del modelo de esteganográfia planteado para dispositivos móviles.

### 3.1. Filtros

A continuación se describen los filtros aplicados a la información para su procedente ocultamiento. La información a procesarse se divide en dos categorías: información entrante e información generada. La información entrante hace referencia la información ingresada por el usuario, primordialmente el mensaje que se desea enviar y la selección del algoritmo esteganográfico a utilizar. La información generada es información producto de los procesos aplicados a las diferentes variables manipuladas al interior del programa.

**Figura 7. Encabezado utilizado por EstegoMovil.**

| Bandera Tipo esteganografia | Tamaño mensaje | Fotografía | |
|---|---|---|---|
| | | Ancho | Alto |
| 1 Bits | 8 Bits | 8 Bits | 8 Bits |

Una vez aplicados los filtros respectivos se crea el encabezado tomando como base el orden y numero de máximo de bits que se pueden utilizar para describir el contenido de cada campo (figura 7).

Dicho encabezado será utilizado para todo proceso de ocultamiento y será lo primero en ingresar y salir de la imagen portadora. Esto se debe a que sin la información contenida en el encabezado, es imposible iniciar el procesador esteganográfico.

#### 3.1.1. Información entrante

Mensaje: Es el mensaje que se desea ocultar al interior de la imagen portadora.

- Se aplica filtro de tamaño para contabilizar la cantidad de letras que componen el mensaje para luego convertir el valor obtenido a su representación binaria de 8 bits[3]. La representación binaria obtenida es almacenada en el campo *Tamaño mensaje* del encabezado.

Selección algoritmo esteganográfico: Indica el algoritmo utilizado para realizar el proceso de ocultamiento sobre la imagen portadora.

- El valor del campo *Tipo esteganográfia* del encabezado será cero (0) si se utilizo el Algoritmo Esteganográfico Seguro, uno (1) si se utilizo el Algoritmo Esteganográfico Simple.

#### 3.1.2. Información generada

Dimensiones: Dimensiones de Ancho y Alto de la fotografía portadora. Las dimensiones son necesarias para reconstruir la foto cuando arriba al receptor.

- Se aplica filtro para obtener el ancho de la fotografía. El valor obtenido es convertido a su representación binaria de 8 bits. La represesentación obtenida es almacenada en el campo Fotografía/Ancho del encabezado.

- Se aplica filtro para obtener el alto de la fotografía. El valor obtenido es convertido a su representación binaria de 8 bits. La represesentación obtenida es almacenada en el campo Fotografía/Alto del encabezado.

### 3.2. Algoritmos Esteganográficos

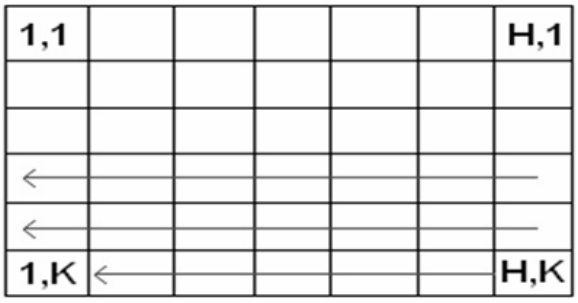
Como núcleo fundamental del modelo para la transmisión de información oculta a través de dispositivos móviles se proveen dos algoritmos esteganográficos encargados de realizar el proceso de fusión entre la imagen portadora y el mensaje huésped. El primer algoritmo utiliza un modelo de ocultamiento lineal secuencial. El segundo utiliza el modelo de ocultamiento pseudo aleatorio dependiente de una llave. Si bien su funcionamiento es diferente, el núcleo procesal realiza el mismo procedimiento, IBMS (Inserción en BIT menos significativo). Gracias a este núcleo común, los filtros aplicados a la información a ocultar, así como a la imagen capturada son comunes para los dos algoritmos.

3.Utiliza corrimiento de bits para cada valor que se desea convertir. Bit = valor & ( 1 << j ) para 1< j < 8

### 3.2.1. Algoritmo esteganográfico Simple

Basado en el modelo de ocultamiento secuencial lineal, el algoritmo oculta información en píxeles linealmente contiguos (seguidos) en la superficie de la imagen.

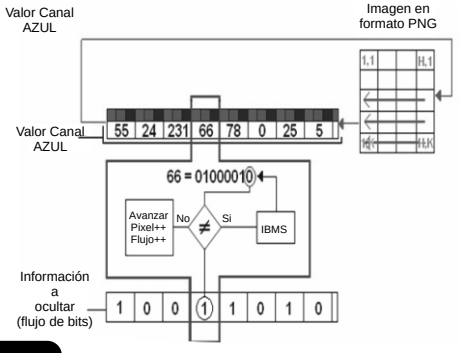
**Figura 8. Recorrido secuencial realizado por el algoritmo esteganográfico simple.**




Como punto de partida del algoritmo se selecciona el píxel ubicado en la posición P(H,K), ultimo píxel de la imagen. A partir de este píxel, y desplazándose de forma secuencial inversa (H, H-1, H-2, H-3 ... 1) se procede a realizar el proceso IBMS sobre cada píxel, tantas veces como bits tenga el mensaje[4]. Una vez recorrida la totalidad de píxeles de una fila ( P(H,K), P(H-1,K), P(H-2,K) ... P(1,K) ) el algoritmo disminuye K para reiniciar el proceso sobre la fila anterior (K, K-1, K-2, ... 1) Dicho procedimiento se hará tantas veces como filas se ocupen en el ocultamiento o recuperación del mensaje.

Si el modulo de procesamiento esteganográfico se encuentra operando en modo recepción, el encabezado será el primer trozo de información recuperado de la imagen portadora. Utilizando los valores al interior del encabezado como valores de inicialización se procede a iniciar la ejecución del algoritmo. Uno a uno se recorre los píxeles de forma secuencial (Figura 8) hasta recorrer tantos píxeles como cantidad de bits contenía la representación binaria del mensaje oculto. A medida que se recuperan los bits, se construyen paquetes de 8 bits los cuales construyen una letra del mensaje. Una vez finalizado el proceso inverso se cuenta con un mensaje legible el formato UTF8.

**Figura 9. Algoritmo esteganográfico simple**

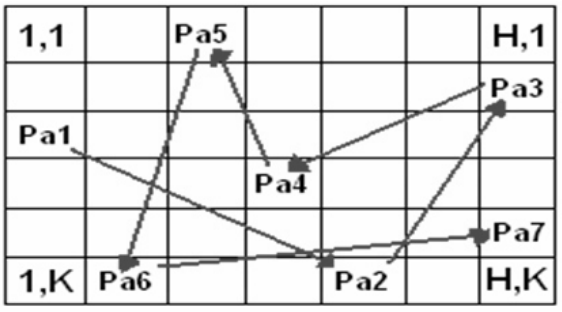



Por el contrario, si el procesador esteganográfico se encuentra operando en modo envío, el flujo de información a ocultarse estará conformado, en este orden, por encabezado y mensaje; los dos como una representación binaria de la información que alojan. Dicho flujo de bits ingresa al procesador esteganográfico (el algoritmo) el cual recorre de forma simultanea los bits del flujo y los píxeles de la fotografía. Uno a uno compara el BMS del canal azul del píxel con el BIT en la posición que se esta leyendo en el flujo de bits. Si el BMS del canal azul del píxel coincide con el BIT del flujo entonces no realiza cambio alguno y pasa al siguiente BIT del flujo y al siguiente píxel. Por el contrario, si el BMS del canal azul del píxel no coincide con el BIT del flujo, el procesador esteganográfico, a través de IBMS, iguala el BMS del canal azul del píxel con el BIT al interior del flujo (Figura 9). Dicho procedimiento es iterado tantas veces como bits tenga el flujo de bits.

### 3.2.2. Algoritmo esteganográfico seguro

Basado en el modelo de ocultamiento pseudo aleatorio iniciado por llave. El algoritmo oculta información en píxeles seleccionados a través de un generador de coordenadas aleatorias que utiliza como base para funcionar una llave/semilla. El tamaño del mensaje varía de 1 a 250(tamaño máximo del mensaje) lo cual genera 250 caminos aleatorios distintos para ocultar la información sobre la superficie de la imagen (Figura 10). Dicho análisis desemboca en la escogencia del tamaño del mensaje como llave para iniciar el generador aleatorio.

**Figura 10. Recorrido aleatorio sobre la superficie de la imagen.**




El algoritmo utiliza un generador de coordenadas aleatorias de carácter deterministico[5], el cual siempre genera una misma secuencia de números para una misma semilla ingresada. Como medida para evitar daños en la información ya oculta, se crea un evaluador de números aleatorios repetidos.

4.Numero de letras del mensaje x 8 = número de bits que componen el mensaje en su representación binaria.
5.Para una X semilla ingresada, el generador de número aleatorios genera siempre la misma secuencia de números.

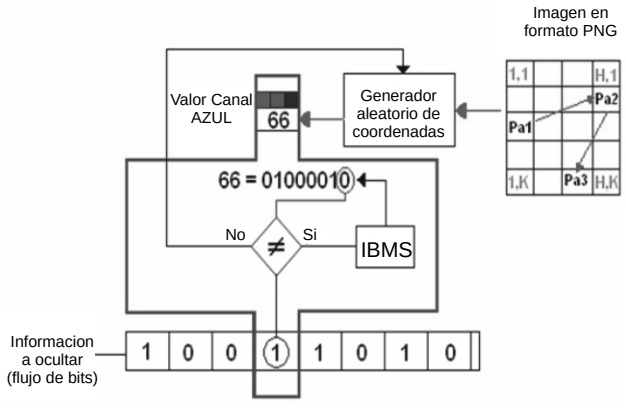
La función del evaluador es verificar que el número generado de forma aleatoria no haya sido utilizado en el proceso de ocultamiento.

Si el modulo de procesamiento esteganográfico se encuentra operando en modo recepción, el encabezado será el primer trozo de información recuperado de la imagen portadora. Utilizando los valores al interior del encabezado se procede a iniciar el generador de coordenadas aleatorias así como la ejecución del algoritmo. Para cada coordenada generada se obtiene un bit que compone el mensaje. Se generaran tantas coordenadas aleatorias como cantidad de bits contenía la representación binaria del mensaje oculto. El mensaje es construido siguiendo el mismo procedimiento descrito para el algoritmo esteganográfico simple.

Por el contrario, si el procesador esteganográfico se encuentra operando en modo envío, el flujo de información a ocultar se encuentra conformado por encabezado y mensaje, en este orden; los dos como una representación binaria de la información que alojan. Para ocultar el encabezado del mensaje se utiliza un esquema de ocultamiento secuencial, similar al utilizado por el algoritmo esteganográfico simple. La razón de dicho esquema se fundamenta en la necesidad que tiene el receptor por recuperar el encabezado.

Terminado el ocultamiento del encabezado se procede a ocultar el flujo de bits correspondiente al mensaje. Dicho flujo de bits ingresa al procesador esteganográfico (el algoritmo) el cual recorre de forma secuencial los bits del flujo pero de forma aleatoria los píxeles de la fotografía. El proceso de IBMS utilizado es el mismo descrito para el algoritmo simple pero con una única diferencia. La siguiente posición a utilizarse en el ocultamiento no es seleccionada de forma secuencial, por el contrario, es obtenida utilizando el generador de coordenadas aleatorio (Figura 11). Dicho procedimiento es iterado tantas veces como bits tenga el flujo de bits.

**Figura 11. Algoritmo esteganográfico seguro.**




## 4. CONCLUSIONES

Se abre la posibilidad de ofrecer soluciones de seguridad informática basadas en esteganográfia para el mercado de los dispositivos móviles celulares.

Se provee un modelo de captura, procesamiento y envío migrable a cualquier otro tipo de dispositivo móvil que cuente con una cámara fotográfica y forma de comunicación hacia una red.

Se ofrece una solución tecnológica y económicamente viable para el aseguramiento y transporte de información sensible a través de la red móvil celular.

Se construyo un prototipo que implementará el modelo propuesto en el capitulo III que realiza esteganográfia entre dispositivos móviles y mostró ser 100% funcional.

El prototipo implementado es innovador gracias a las funcionalidades esteganográficas provistas, hasta ahora desconocidas en el ámbito de los dispositivos móviles celulares.

El prototipo es comercialmente rentable. Gracias a la masificación de la telefonía móvil celular, se cuenta con millones de clientes potencialmente interesados en formas de asegurar información sensible.

## 5. REFERENCIAS

[1]Kessler, Gary C. An Overview of Steganography for the computer Forensics Examiner. http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm [En línea]. Forensic Science Communications. Julio de 2004. [Consulta: 17 de febrero de 2007].

[2]Kessler, Gary C. Steganography: Hiding Data Within Data. http://www.garykessler.net/library/steganography. html [En línea]. Data-Hiding. Septiembre de 2001. [Consulta: 20 de mayo de 2007].

[3]Blinn, James F. What Is a Píxel?. http://doi.ieeecomputersociety.org/10.1109/MCG.2005.119 [En línea]. IEEE Computer Society. Septiembre/Octubre 2005. [Consulta: 20 de mayo de 2007].

[4]Johnson D. Transformada Discreta de Fourier (DFT). http://cnx.org/content/m12844/1.1/ [En línea]. Junio de 2005. [Consulta: 20 de mayo de 2007].

[5]Fusión de imágenes mediante Transformada Wavelet Diatica. http://cpdsi-fich.wikidot.com/local--files/tpsaplicacion/2006_Fortonani-Fusion.pdf [En línea]. Captura y procesamiento digital de señales e imágenes. [Consulta: 20 de mayo de 2007].

[6] Guillermo[6]. A few thoughts about steganography.

6. Pseudónimo del autor del artículo.

http://www.guillermito2.net/stegano/ideas.html [En línea]. [Consulta: 20 de mayo de 2007].
[7]Upham, Derek. JSTEG *Does not Read JPEG Files. http://packetstorm.ussrback.com/crypt/stego/DOS/jsteg.txt [En línea]. Packer Storm. Diciembre de 1999. [Consulta: 20 de mayo de 2007].
[8]Asahi, Net. Form Mime Type List. http://www.asahi-net.or.jp/en/guide/cgi/mimetype.html [En línea]. ASAHINet Inernet Service Provider & Community. [Consulta: 20 de mayo de 2007].
[9]Fujitsu. Sobre Nosotros: Fujitsu Services S.A. http://www.fujitsu.com/es/about/ [En línea]. Fujitsu, The Posibilities are Infinite. [Consulta: 20 de mayo de 2007].
[10]Fujitsu Laboratories. Steganography Code Recognition Technology. http://jp.fujitsu.com/group/labs/downloads/en/business/activities/activities-4/fujitsu-labs-imagevoice-003-en.pdf [En línea]. Fujitsu, The Posibilities are Infinite. Julio de 2005. [Consulta: 20 de mayo de 2007].
[11]Dunbar, Bred. A Detailed Look at Steganographic Techniques and their use in an Open-Systems Enviroment.
http://www.sans.org/reading_room/whitepapers/covert/677.php [En línea]. SANS Institute. Enero de 2002. [Consulta: 20 de mayo de 2007].
[12]Ortiz, C. Enrique. The Wireless Messaging API 2.0. http://developers.sun.com/techtopics/mobility/midp/articles/wma2/index.html [En línea]. Sun Developer Networks. Octubre de 2005. [Consulta: 20 de mayo de 2007].
[13]Ortiz, C. Enrique. The MIDP 2.0 Push Registry. http://developers.sun.com/techtopics/mobility/midp/articles/pushreg/ [En línea]. Sun Developer Network. Junio de 2003. [Consulta: 20 de mayo de 2007].
[14]Mahmoud, Qusay. H. The J2ME Mobile Media Api. http://developers.sun.com/mobility/midp/articles/mmapioverview/index.html [En línea]. Sun Developer Network. Junio de 2003. [Consulta: 20 de mayo de 2007].
[15]Menezes, Alfred J.; Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography. http://www.cacr.math.uwaterloo.ca/hac/ [En línea]. Center for applied cryptographic research. Agosto de 2001. [Consulta: 20 de mayo de 2007].